SOLUTION BRIEF

Contrast Application Detection and Response (ADR) and IBM QRadar SIEM

Enhance threat detection within IBM QRadar SIEM

Gain accurate insights and control over application security incidents directly within the IBM QRadar SIEM console. The Contrast ADR integration equips Security Operations Centers (SOCs) with unparalleled visibility into application and API threat activity, transforming how QRadar environments manage this critical risk vector. By embedding precise, actionable intelligence from deep within applications into QRadar, Contrast ADR enables faster, more accurate threat detection and response, optimizing SOC resources.

The application risk blind spot in the SOC

Security teams face persistent challenges in effectively managing threats targeting the application layer. Ambiguous alerts from perimeter tools like the WAF often trigger alerts that lack the necessary context for efficient investigation, consuming valuable analyst time and potentially obscuring genuine threats. Without direct insight into application behavior, accurately assessing the risk associated with specific alerts or correlating application-level compromises with broader network activity is difficult. This visibility gap represents a significant unmanaged risk and operational drag, hindering the SOC's ability to protect critical business assets delivered via applications and APIs.

Precise application context, integrated with QRadar

Contrast ADR enhances IBM QRadar SIEM investigation workflows by enriching offenses with high-fidelity application attack details unavailable through other means. By instrumenting applications and APIs, Contrast delivers accurate intelligence about exploits, probes, and anomalies directly into the QRadar data pipeline. This allows QRadar's advanced correlation engine to function with greater precision, linking application security events to other indicators across the infrastructure. Analysts gain immediate access to crucial context, such as exact code vulnerabilities and attack payloads, directly within QRadar offenses. Additionally, Contrast's built-in runbooks measurably improve response metrics by offering guided triage, standardizing response procedures, and accelerating containment actions for specific application attack types.

This deep integration empowers SOC teams using QRadar to:

Enhance threat detection accuracy

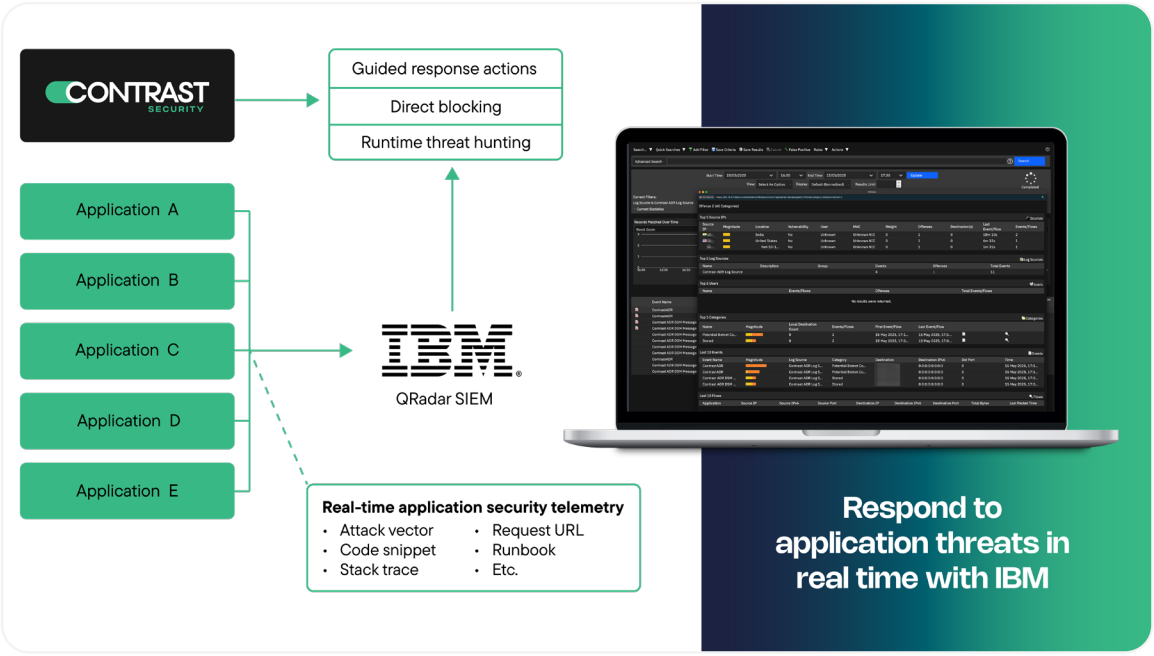
Leverage precise alerts based on direct application activity to effectively prioritize critical threats and reduce false positives.

Accelerate response with context

Enrich QRadar security investigations with deep application context, like specific lines of code impacted, for faster threat analysis and response.

Gain actionable insights

Correlate security events with direct observations from within the application to understand the complete attack chain.



Optimizing QRadar for application security use cases

Accelerating application incident closure within QRadar

Challenge: Application-related QRadar Offenses often suffer from long resolution times due to insufficient data for rapid root cause analysis and remediation validation.

Solution: Contrast ADR delivers definitive application context directly into QRadar. This detailed intelligence within Offenses, combined with guided steps in the provided runbooks, enables analysts to quickly understand the attack, validate remediation, and demonstrably reduce Mean Time To Resolution (MTTR) for application security incidents.

Detecting evasive threats targeting critical applications

Challenge: Sophisticated attackers leverage unknown vulnerabilities (zero days) or hide within legitimate application functions, bypassing traditional detection capabilities feeding into QRadar.

Solution: Contrast ADR's detection approach identifies malicious behavior patterns within applications, regardless of known signatures. Feeding this unique intelligence into IBM QRadar SIEM allows the correlation engine to flag suspicious activities that would otherwise remain invisible, enabling timely response to evasive threats.

Enabling proactive application threat discovery with QRadar

Challenge: Identifying hidden compromises or assessing the true scope of an application breach requires deep visibility often lacking in standard QRadar data sources.

Solution: Contrast ADR provides rich telemetry on internal application activity. Analysts can leverage this data within IBM QRadar SIEM, utilizing its powerful search features (including AQL), to proactively hunt for subtle indicators of compromise, map attacker pathways, and fully understand the impact of application-focused campaigns.

Ready to see Contrast in action?

Visit our website or request a demo today to learn how Contrast Security can empower your IBM Qradar environment with deep application security insights.

Try Contrast

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333